Segurança em Dispositivos Móveis: Um Estudo Sobre a Adoção de Boas Práticas para Proteção em Celulares

Juliana Pereira Cabral[1], Herleson Paiva Pontes[1]

[1]Grupo de Pesquisa em Informática Aplicada, Redes e Telecomunicações (IART)
Curso Superior de Tecnologia em Redes de Computadores
Instituto Federal do Ceará (IFCE) – Jaguaribe – CE – Brasil

{julianajbe2102,herleson}@gmail.com

Abstract. *In recent years, it is remarkable the increase of cybersecurity attacks on mobile devices in Brazil, where was estimated more than 850 thousand attempts aiming at improper access to users' personal data. This paper presents a study about the adoption of security features, tools and best practices at smartphones. After conducting a case study with 222 participants that evaluated technological and psychological aspects of users about their cellphones safety, the results suggest that a considerable portion of the population has little knowledge about the use of resources and practices for efficient protection in mobile devices, making them cybercrime targets.*

Resumo. *Nos últimos anos, é possível observar o considerável aumento do número de ataques à segurança da informação em dispositivos móveis no Brasil, onde estima-se que ocorreram 850 mil tentativas objetivando o acesso indevido aos dados pessoais dos usuários. Este trabalho apresenta um estudo sobre a adoção dos recursos, ferramentas e boas práticas de segurança voltadas para celulares. Após a condução de um estudo de caso envolvendo 222 participantes que avaliou aspectos tecnológicos e psicológicos dos usuários acerca da segurança em seus aparelhos, os resultados sugerem que parcela considerável da população possui escasso conhecimento em relação ao emprego dos recursos e boas práticas de proteção eficientes nos dispositivos móveis, tornando-os alvos de crimes cibernéticos.*

1. Introdução

Diante dos avanços tecnológicos recentes, é possível observar o aumento do uso de dispositivos móveis, com destaque dos celulares, graças a sua portabilidade, praticidade e capacidade de exercer funções semelhantes às de um computador pessoal. No Brasil, de acordo com a Anatel em 2020 o Brasil teve 234 milhões de acessos a dispositivos móveis, cerca de 7,39 milhões a mais em relação a 2019 [VALENTE, 2021].

Neste cenário, por tratar-se de um dispositivo utilizado no dia-a-dia das pessoas, os celulares comumente armazenam informações pessoais e corporativas, muitas delas classificadas como sensíveis/confidenciais [CERT.br 2020]. Esse comportamento acaba contribuindo para que cibercriminosos realizem ações maliciosas que buscam explorar vulnerabilidades nesses equipamentos e acessar os dados dos usuários. Estima-se que, no ano de 2020 houve um crescimento de 124% de ataques a dispositivos móveis, especialistas acreditam que o trabalho remoto e os links compartilhados via *WhatsApp* usando o Covid-19 tenham grande parcela disso [RODRIGUES, 2020].

Apesar do crescente número de ataques, os celulares ainda não recebem a devida atenção em relação a sua segurança por parte de seus usuários [Roshandel, Arabshahi e Poovendran 2013]. É notória a diferença dos cuidados com a segurança dos celulares em comparação com os computadores pessoais. Portanto, empregar recursos, ferramentas e boas práticas que visam a proteção dos celulares e de seus dados são essenciais para a redução da probabilidade desses equipamentos se tornarem alvos de ataques, impedindo assim que informações sejam acessadas indevidamente [Cavalcanti 2016].

Embora exista um número considerável de pesquisas voltadas para a segurança em celulares, evidências sugerem que são poucas as contribuições que determinam quais boas práticas de segurança devem ser adotadas pelos usuários que objetivam proteger seus dados. Além disso, aspectos psicológicos e comportamentais do usuário também contribuem para que a proteção nos ambientes móveis se torne ainda mais desafiadora.

Neste contexto, este artigo descreve um estudo sobre a adoção dos recursos, ferramentas e boas práticas de segurança voltadas para aparelhos celulares, avaliando os recursos empregados, verificando os níveis de proteção adotados e estabelecendo um comparativo entre as ações adotadas e àquelas recomendadas pelos profissionais de segurança da informação. A avaliação foi realizada nos contextos quantitativo e qualitativo, objetivando mostrar a relação entre a adoção de boas práticas e o nível de segurança dos celulares, nas perspectivas técnica e psicológica.

2. Trabalhos Relacionados

São diversos os estudos relacionados à área de segurança da informação voltado para dispositivos móveis, demonstrando o alto interesse da comunidade científica pela temática. Uma das linhas de pesquisa nesta área concentram os trabalhos que analisam os riscos existentes nos ambientes computacionais, com suas respectivas probabilidades e impactos para os usuários de celulares. Estudos como os de Goel e Jain [2017], Amaral *et al.* [2017], Atkinson *et al.* [2016], e Park *et al.* [2014] abordam vulnerabilidades ocasionadas por aspectos técnicos e humanos, demonstrando a complexidade inerente os estudos em segurança da informação.

Estudos mais recentes sobre a Segurança da Informação em *smartphones* têm citado o isolamento social por conta do Covid-19 e o consequente aumento do uso desses dispositivos para novas aplicações como motivadores do crescimento no número de ataques. Para Cardoso [2020], a criminalidade digital não é tratada como assunto importante e relevante no país, o que aumenta a probabilidade de sucesso dos ataques à segurança da informação. A autora cita em seu trabalho o exemplo da campanha *#WashYourCyberHands* (*Lave suas Mãos Cibernéticas* em tradução livre), que tem como objetivo divulgar boas práticas de segurança da informação em tempos de pandemia através de cartilhas que poderiam ser distribuídas no Brasil, tendo em vista que algumas pesquisas e iniciativas relacionadas à pandemia acabam sendo usadas pelos cibercriminosos na criação de ataques através de links fraudulentos.

Adicionalmente, existem várias pesquisas que avaliam a eficácia dos recursos de segurança disponíveis para celulares, objetivando averiguar os limites dessa proteção e propor melhorias a essas funcionalidades. Pennekamp, Henze e Wehrle [2017], Harbach, Luca e Egelman [2016], e Khan e Shah [2016] apresentam em seus trabalhos

diversas análises acerca de ferramentas voltadas para a segurança da informação em dispositivos móveis, identificado os níveis de proteção oferecidos e suas contribuições como mecanismo de segurança eficientes.

Outra linha de atuação dos pesquisadores é a proposta de soluções computacionais, boas práticas e diretivas que ampliam a proteção dos celulares e reduzem as chances desses dispositivos serem invadidos. Como pode-se observar nos trabalhos de Pieterse, Oliver e Heerden [2018], Bitton *et al.* [2017], e Cavalcanti [2016] discorrem sobre estratégias para a segurança em dispositivos móveis, tanto na perspectiva da tecnologia como também de comportamentos e atitudes dos usuários.

3. Segurança da Informação em Dispositivos Móveis

Embora existam diferentes definições para a área de Segurança da Informação propostas por diversos autores e pesquisadores, todas elas compartilham como características centrais a preocupação na proteção aos dados, a promoção da continuidade do negócio e a redução dos riscos envolvendo pessoas, equipamentos e processos. Nesta perspectiva Stallings, Bressan e Barbosa (2015) citam que qualquer sistema computacional é considerado seguro caso seja possível identificar a presença de fundamentos básicos relacionado ao controle da proteção, apresentados e significados conforme a Tabela 1.

Tabela 1. Fundamentos de Segurança da Informação

Característica	Descrição	Se Ausente...
Confidencialidade	A informação será acessada apenas por pessoas com autenticação, evitando assim sua perda ou divulgação indevida.	A informação vai estar acessível para qualquer pessoa, mesmo que ela não tenha permissão.
Integridade	A informação não será alterada durante seu transporte por pessoas sem permissão.	As informações podem ser modificadas antes do envio, prejudicando o remetente.
Disponibilidade	O usuário autenticado terá acesso à informação quando necessário, sem nenhuma interrupção.	O usuário não consegue ter acesso à informação a partir de seu dispositivo.
Autenticidade	Garante que a pessoa que está tendo acesso à informação é quem ela diz ser.	Qualquer pessoa terá acesso a informações sem precisar colocar login e senha.
Tempestividade	Conceito genérico que engloba recursos de marcação temporal nas informações geradas/manipuladas.	Não terá a datação eletrônica das informações. O usuário não saberá quando ela foi criada/enviada.
Não-Repúdio	O autor de qualquer ação feita com a informação deve confirmar seus atos e autorias.	Invasores poderão fazer ações maliciosas sem ser descobertos, pois não terá identificação de suas ações.

Uma das linhas de ataques à segurança da informação é representada pelos *malware*, que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em qualquer dispositivo eletrônico, podendo executar ações em nome dos usuários [CERT.br 2017]. São exemplos de malware *vírus*, *worm*, *spyware*, *bot*, *backdoor*, *trojan* e *rootkit*.

Outros tipos de ataques empregam técnicas para conseguir acesso não-autorizado a informações diversas do usuário, tais como aquelas que induzem o usuário a fornecer informações sensíveis e as que empregam engenharia social para ações persuasivas [Stallings 2015]. Exemplos desses ataques são *spoofing*, *sniffing*, *denial of service*, *phishing*, *pharming* e *hijacking*.

Neste contexto, os celulares são um dos alvos favoritos de ataques, pois eles consolidam a execução de atividades profissionais e pessoais em um único equipamento, reúnem grande quantidade de informações armazenadas, possuem maior possibilidade de perda e furto, apresentam considerável número de aplicações desenvolvidas por terceiros e são substituídos rapidamente pelos usuários [CERT.br 2017].

Frente a esse cenário, faz-se necessário o conhecimento das diversas ferramentas e diretivas que promovam a segurança da informação em dispositivos móveis para seus usuários. Destaca-se que, apesar do grande número de soluções disponíveis para a proteção de celulares, todas as formas existentes apresentam pontos falhos. Assim, recomenda-se a utilização combinada de duas ou mais práticas de segurança em um único equipamento, criando camadas adicionais de proteção entre o criminoso e os dados.

4. Visão Geral do Projeto

Para compreender a percepção dos usuários acerca os recursos e boas práticas para a proteção de celulares, este trabalho tem como objetivo principal entender quais formas de proteção voltadas para dispositivos móveis estão sendo utilizadas pelos usuários e as motivações por trás dessas adoções, além de estabelecer uma relação entre os tipos de proteção adotados e os níveis de segurança recomendados para esses equipamentos.

4.1. Método

Em relação à sua finalidade, a pesquisa proposta é definida como aplicada, pois, é utilizada no estudo de um problema em um determinado contexto, buscando soluções nesse ambiente [Wazlawick 2014]. Este trabalho busca identificar ações executadas pelos usuários para proteger seus celulares, baseando-se no conhecimento ao mundo real.

Quanto a seus objetivos, a pesquisa é caracterizada como descritiva, uma vez que busca descrever as características de uma população ou um fenômeno, além de identificar se há relação entre o que está sendo analisado [Wazlawick 2014]. No estudo, encontram-se descritos pontos positivos e negativos das formas como os usuários protegem seus celulares e o que eles realizam que os deixam expostos a ameaças virtuais.

A análise dos dados foi realizada por meio de um estudo de caso que possibilitou a pesquisa quali-quantitativa, pois utiliza tanto a análise qualitativa para descrever o

objeto de estudo com mais profundidade como a pesquisa quantitativa na quantificação para coletar e depois tratar os dados obtidos [Wazlawick 2014].

Por fim, esta pesquisa é classificada como de levantamento, pois utiliza questionário para obter os dados que permitem identificar padrões e tendências sobre grupos de pessoas e, assim, entender melhor seus comportamentos [Wazlawick 2014].

4.2. Processo de Desenvolvimento

No primeiro estágio da pesquisa, realizou-se estudos para apropriação das dos diversos tópicos que fundamentam a área de segurança da informação. Foram feitos levantamentos sobre fundamentos de sistemas de informação, princípios de segurança da informação e segurança da informação em celulares. Foram analisados artigos publicados em periódicos, trabalhos em conferências científicas e livros, nos idiomas Inglês e Português.

Com base no levantamento realizado, a etapa seguinte consistiu na criação do estudo de caso, que teve como objetivo conhecer quais os métodos de segurança utilizados pelos usuários em seus celulares e quais ações essas pessoas realizam que as tornam alvos de ataques cibernéticos. Também foram escolhidos para análise alguns aspectos psicológicos relacionados à forma como o usuário sente-se seguro ou inseguro com suas escolhas de métodos de segurança. Utilizou-se um questionário para a coleta dos dados junto aos participantes do estudo de caso.

A terceira etapa consistiu na aplicação do questionário, através de uma plataforma *online*. A distribuição do link entre os participantes ocorreu através de diversos meios de comunicação, como compartilhamento entre grupos de redes sociais, apresentação do link em plataformas acadêmicas e envio por e-mail.

Na fase subsequente, realizou-se a análise dos dados coletados para a obtenção dos resultados qualitativos e quantitativos. Neste momento, os dados coletados foram tabulados e estruturados para a visualização clara das informações geradas, de tal modo que foram realizadas reflexões sobre as constantes e variáveis informadas pelos usuários.

Na última etapa do projeto, discorreu-se sobre os métodos de segurança mais e menos utilizados pelos entrevistados, seus pontos fortes e fracos à luz das diretivas de segurança da informação. Além disso, foram apresentadas reflexões sobre as impressões que os usuários têm sobre segurança da informação e os riscos dessas atitudes.

5. Estudo de Caso

Para a realização do estudo de caso foi escolhido o método da aplicação de um questionário *online*, cuja elaboração dos itens foi embasada nos fundamentos de segurança da informação como mostrado na Tabela 1, com ênfase em aparelhos celulares. Ao todo, o questionário contém 22 (vinte e duas) perguntas, distribuídas entre objetivas e discursivas, agrupadas conforme a temática abordada por cada item.

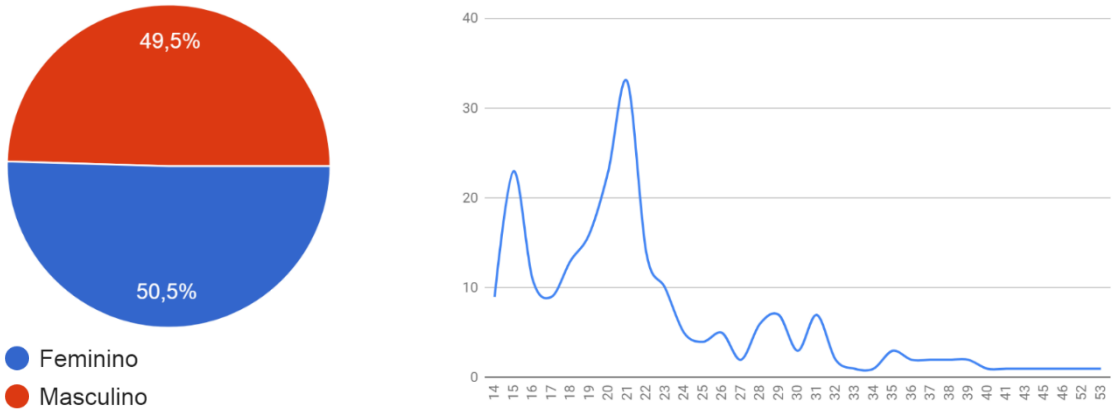
Os itens coletaram dados relacionados aos diversos tipos de proteção disponíveis nos celulares e suas utilizações pelo usuário, avaliaram aspectos psicológicos quanto a satisfação do usuário com a segurança do seu dispositivo móvel, e propuseram reflexões discursivas sobre aspectos técnicos e psicológicos no ponto de vista do usuário. Em linhas gerais, foram feitas perguntas sobre as seguintes temáticas:

- *Ferramentas para Bloqueio de Tela:* O bloqueio de tela é a forma de proteção mais usada pelos usuários de celulares. Por isso buscou-se identificar informações sobre quais tipos de bloqueio eram os mais utilizados e seus níveis de segurança.
- *Senhas:* Como este recurso oferece acesso a todas as plataformas/soluções que armazenam e manipulam dados, a gestão de senhas é uma complexa tarefa. Foram coletadas informações sore critério de escolha, composição, frequência de mudança e armazenamento das senhas dos usuários.
- *Sistema Operacional e Aplicativos de Segurança:* Boa parte dos recursos de segurança disponíveis para os usuários são implementados na forma de aplicativos e ferramentas do próprio sistema operacional. Questionou-se aos participantes sobre o uso de antivírus, instalação de aplicativos e de ações no nível de administrador.
- *Percepção do Usuário:* Os usuários esperam que seus dispositivos estejam seguros, mas muitos deles não procuram aprender e utilizar recursos que aumentem a segurança dos seus dispositivos móveis. Portanto, foram elencadas questões sobre a sensação de segurança do usuário, sobre como ele(a) se sente quando encontra-se longe do celular, e quando uma outra pessoa está usando seu aparelho.

6. Resultados e Discussão

6.1. Resultados

O estudo de caso contou com o total de 222 (duzentos e vinte e dois) participantes, sendo 112 (cento e doze) mulheres (50,5%) e 110 (cento e dez) homens (49,5%). A média de idade dos participantes foi de 22,37 anos, com moda igual a 21 anos e mediana também igual a 21 anos, conforme Figura 1.



(a) **(b)**

Figura 1. Distribuição da amostra do estudo por (a) gênero e (b) faixa etária

Os níveis de escolaridade dos entrevistados foram: “Ensino Fundamental Completo”: 5,4%; “Ensino Fundamental Incompleto”: 0,9%; “Ensino Médio Completo”: 22,5%; “Ensino Médio Incompleto”: 16,7%; “Ensino Superior Completo”: 18%; e “Ensino Superior Incompleto”: 36,5%.

Nas perguntas sobre as ferramentas para bloqueio de tela, observou-se que a maioria dos usuários utiliza a “Impressão Digital” como principal recurso com 33,8%,

seguido do “Padrão de Desenho” com 28,4%. Também chamou a atenção o fato de alguns participantes afirmarem que não utilizam qualquer tipo de bloqueio (13,6%).

Nos questionamentos acerca da senha empregada nos celulares e aplicativos instalados, foi possível observar comportamentos interessantes por parte dos participantes. Mais de 1/3 dos entrevistados afirmam usar a mesma senha para todos os aplicativos e plataformas *online* (34,2%); “número” e “letras minúsculas” são os caracteres mais empregados nas senhas de 2/3 da amostra (77,9% e 67,6% respectivamente); “data especial” é a informação pessoal mais usada em senhas (40,1%); a maioria dos entrevistados costuma salvar as senhas nos celulares (58,1%); considerável parte dos participantes não possuem o hábito de alterar suas senhas (45,5%), ilustrado na Figura 2; e quase metade disseram empregar informações pessoais na composição das senhas (49,1%), conforme mostra a Figura 3.

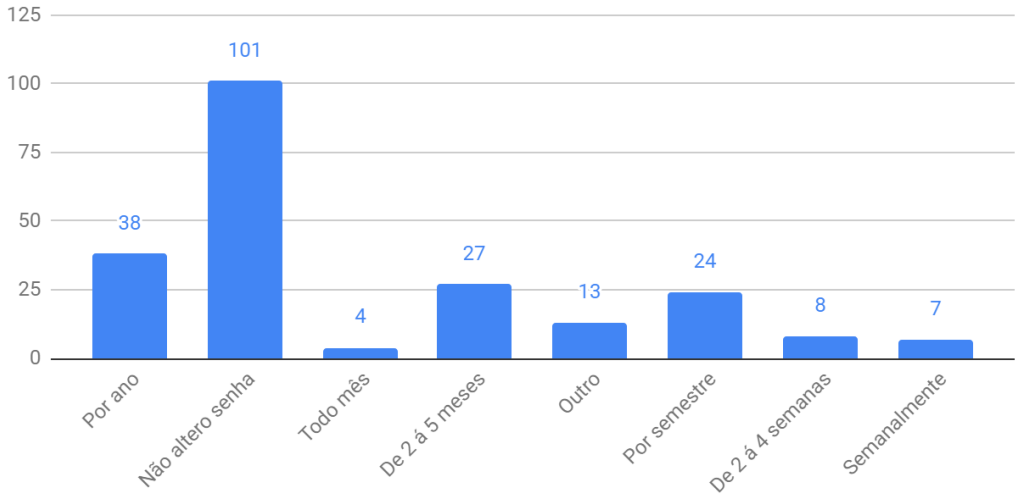


Figura 2. Distribuição sobre a frequência de alteração da senha pelo usuário

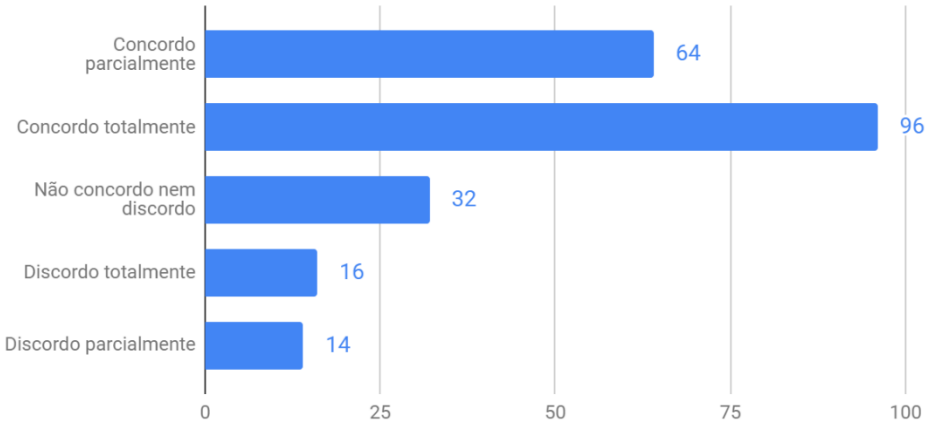


Figura 3. Distribuição sobre o uso de informações pessoais nas senhas

Sobre as questões de segurança relacionadas ao sistema operacional e aplicativos instalados, percebeu-se diferenças notórias entre o comportamento do usuário no celular quando comparado com o comportamento nos computadores pessoais. Aplicativos do tipo “antivírus” ainda não são empregados em celulares por 63,5% dos participantes, 49,5% conhecem o recurso de acessar o celular como administrador do sistema (root) e enxergam a ação como benéfica para o aparelho. A imensa maioria dos entrevistados

(69,1%) afirmaram instalar aplicativos que não são das lojas oficiais. O emprego da computação em nuvem também chamou a atenção durante o estudo de caso, uma vez que 51,4% dos participantes conhecem a tecnologia e a utiliza no seu dia-a-dia.

Por fim, os dados coletados a partir dos itens relacionados à percepção do usuário com relação ao seu sentimento de segurança trouxeram à tona informações interessantes para reflexão. Para 45.5% dos participantes, os recursos de segurança oferecidos pelos celulares protegem apenas parcialmente seus aparelhos, e apenas 11,7% acreditam ter seus celulares completamente protegidos. Este sentimento de insegurança reflete-se no fato de que 67,7% das pessoas entrevistadas afirmarem levarem seus celulares para todos os lugares e recintos que vão, conforme Figura 4.

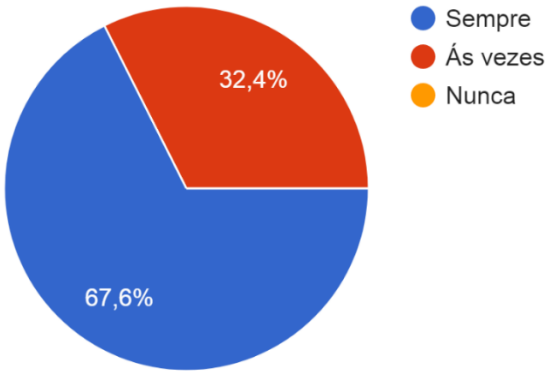


Figura 4. Distribuição sobre a necessidade de levar o celular para todo lugar

Ainda neste sentido, ao serem questionados sobre como se sentem quando não estão próximo do celular, os sentimentos de insegurança dos usuários apareceram em respostas como *"triste"*, *"como se faltasse uma parte de si"* e *"inseguro"*. Os entrevistados também foram sobre como se sentiam quando uma pessoa está utilizando seu celular, onde foram observadas respostas como *"incomodado"*, *"não gosta de emprestar"*, *"medo"*, *"desconforto"* e *"atento"*.

6.2. Discussão

A proposta central desse trabalho é analisar o uso seguro de celulares pelos usuários, sempre em observância com as boas práticas recomendadas. Neste contexto, os resultados apresentados oferecem reflexões interessantes sobre a proteção nesses dispositivos.

Observou-se que os usuários se expõem a ameaças virtuais ao procurar opções de bloqueio de tela que são mais rápidas de se utilizar, mas que não necessariamente são as mais seguras. Também é preocupante observar que boa parte das pessoas consolidam o acesso a toda sua vida digital em uma única senha, pois o invasor terá acesso aos aplicativos, sites e redes sociais do usuário afetado, roubando suas informações e usando-as para diversas ações maliciosas. O uso de informações pessoais na formação das senhas é outro problema encontrado durante o estudo de caso, uma vez que as primeiras tentativas de descobertas de senhas pelos cibercriminosos utilizam essas informações pessoais, muitas delas visíveis em redes sociais e sites públicos.

Ainda sobre as senhas, a composição da palavra-chave carece de cuidado por boa parte dos usuários, pois são poucos os que utilizam letras minúsculas e maiúsculas, números e caracteres especiais na sua elaboração. A combinação desses tipos de

caracteres aumenta substancialmente a sua complexidade, dificultando a ação dos criminosos. A frequência de mudança é outro ponto que necessita de reflexão por parte do usuário, pois mudá-la periodicamente é uma forma de dificultar a descoberta. Este é um hábito que deve ser desenvolvido e estimulado, para que os níveis de proteção sejam mantidos, considerando inclusive problemas de vazamento de dados de grandes plataformas e empresas que ocorrem periodicamente.

Os recursos oferecidos pelo sistema operacional e aplicativos de segurança ainda são desconhecidos de parcela significante dos usuários. Estimular o uso antivírus, instalar aplicativos fornecidos apenas pelas lojas oficiais e evitar a realização do desbloqueio administrativo do celular são essenciais para proteger o aparelho e suas informações.

A possibilidade de ter informações vazadas afeta psicologicamente os usuários de celulares, independentemente dos níveis de segurança oferecidos pelos recursos e boas práticas disponíveis. Aprender e compartilhar conhecimento sobre segurança da informação pode ajudar a melhorar a proteção dos celulares e a satisfação dos usuários, reduzindo o sentimento de insegurança. Adicionalmente, existe atualmente altos níveis de dependência dos usuários com seus aparelhos celulares. Esta proximidade excessiva acaba por reduzir o senso de proteção do usuário: ele(a) acredita que o seu aparelho está, de certa forma, protegido pois o mesmo encontra-se "na palma da sua mão". O emprego dos recursos e boas práticas deve, portanto, ser mandatório para proporcionar níveis adequados de segurança ao seu celular e dados nele contidos.

6.3. Boas Praticas

Com base nos resultados obtidos pelo questionário e na análise realizada nos dados obtidos, é possível propor uma série de boas práticas que pode ser empregada por usuários para que o nível de segurança de suas informações nos *smartphones* seja o mais adequado possível:

- O bloqueio de tela considerado mais seguro é a senha com letras minúsculas, maiúsculas, números e caracteres especiais;
- A combinação de dois fatores de autenticação aumenta a segurança dos aparelhos móveis;
- As senhas não devem construídas com informações pessoais do usuário, devendo optar por palavras e números aleatórios sempre que possível;
- Cada aplicativo/plataforma *online* deve conter uma senha diferente, e evitar seu armazenamento no dispositivo móvel;
- A senha de aplicativos e plataformas digitais deve ser trocada periodicamente, em intervalos de 30 (trinta) a 180 (cento e oitenta) dias, ou quando o usuário perceber que ela pode ter sido descoberta;
- Ao baixar um antivírus, o usuário deve estar atento as avaliações e escolher um que não seja fraudulento, principalmente nas lojas de aplicativos que não possuem verificação dos aplicativos publicados;
- Deve-se evitar o processo de "rootear" o aparelho celular, pois abre margem para a instalação de aplicativos maliciosos que poderão realizar ações irreversíveis no *smartphone*.

- É importante que todos os aplicativos instalados no *smartphone* sejam da própria loja do dispositivo, além de evitar aplicativos de terceiros que não estejam nas lojas oficiais;
- A utilização da computação em nuvem possibilita que o usuário tenha seus dados e arquivos armazenados em uma unidade remota protegido por diversas formas de autenticação/autorização, evitando o armazenamento apenas no próprio dispositivo;
- O emprego de boas práticas e a conscientização dos usuários acerca da importância da segurança da informação proporcionam o sentimento de segurança com seu dispositivo. Esta condição é importante para a manutenção da saúde mental do usuário, pois reduz o sentimento de desproteção e de medo quando ele(a) encontra-se longe do seu aparelho ou quando outras pessoas estão utilizando seu *smartphone*.

7. Considerações Finais

Este projeto avaliou o nível de proteção utilizado por pessoas em seus celulares e identificar, por meio de um questionário, os hábitos prejudiciais que expõem os dados armazenados nesses dispositivos.

De acordo com os dados obtidos no trabalho, pode-se estabelecer um perfil recorrente de usuários que ainda são leigos quando se refere a proteger seu dispositivo. Também observou-se como a percepção psicológica do usuário afeta sua sensação de segurança, pois essa pessoa sente-se insegura quando fica longe do seu aparelho independente dos recursos de segurança utilizados.

Nesse contexto, as descobertas sugerem que, apesar da boa gama de recursos de segurança nos dispositivos móveis, existem potenciais riscos devido à combinação entre o grande volume de informações armazenadas e manipuladas com o uso de escassos recursos de segurança da informação.

Sobre trabalhos futuros, uma alternativa seria a construção de aplicativos que realizem "varreduras" de segurança nos dispositivos, objetivando identificar possíveis melhorias em termos de segurança. Outra proposta de trabalho futuro seria a construção de aplicativos que possibilitem auditar os dados, ou seja, que habilitem o rastreamento dos dados manipulados por usuários e aplicativos via celulares. Adicionalmente, outro possível trabalho futuro é o estudo sobre a influência da idade, grau de instrução e de outras variáveis socioeconômicas no emprego dos recursos e boas práticas em segurança.

Referências

Amaral, G., Silva, R., Rotondo, G. and Amaral, E. (2017) "Um estudo sobre vulnerabilidades do Android: Ferramentas soluções para usuário", SULCOMP.

Atkinson, J. S., Mitchell, J., Rio, M. and Matich, G. (2016) "Your Wi-Fi leaking: What do you mobile apps gossip about you?", In Future Generation Computer Systems.

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L. and Shabtai, A. (2017) "Taxonomy of mobile user´s security awareness", In Computers & Security, v.73.

Cardoso, N. M. A. (2020) "Pandemia do Cibercrime." In Revista Eletrônica Direito & TI, v.1 n. 12.

Cavalcanti, K. R. P. (2016) “Uma solução integrada para a melhoria da segurança de dispositivos móveis baseada na plataforma Android”.

CERT.br. (2020) “Cartilha de Segurança para Internet.” https://cartilha.cert.br/, December/2020.

Goel, D. and Jain, A. K. (2017) “Mobile phishing attacks and defense mechanisms: State of art and open research challenges”, In Computers & Security, v.73.

Harbach, M., de Luca, A. and Egelman, S. (2016) “The anatomy of smartphone unlocking”, In: Human-Computer Interaction, San Jose, CA, USA.

Khan, M. H. and Shah, M. A. (2016) “Survey on security threats of smartphones in internet of things”, In: 22nd International Conference on Automation and Computing, p. 560-566.

Park, M-W, Choi, Y-H, Eom, J- H and Chung, T-M. (2014) “Dangerous Wi-Fi access point: attacks to benign smartphone applications”, In Pers Ubiquit Comput.

Pennekamp, J., Henze, M. and Wehrle, K. (2017) “A survey on the evolution of privacy enforcement on smartphones and the road ahead”, In Pervasive and Mobile Computing, v. 42.

Pieterse, H., Oliver, M. and Heerden, R. V. (2018) “Smartphone data evaluation model: Identifying authentic smartphone data”, In Digital Investigation, v.24.

Rodrigues, R. (2020) “Ataques a dispositivos móveis cresceram 124% em março, https://www.kaspersky.com.br/blog/phishing-covid-smartphone-pesquisa/14663/, May/2021.

Roshandel, R., Arabshahi, P. and Poovendran, R. (2013) “LIDAR: A Layered Intrusion Detection and Remediation Framework for smartphones”, In Proceedings 4th ACM Sigsoft symposium on Architecting critical systems, p. 27-32.

Stallings, W., Bressan, G. and Barbosa, A. (2015) “Criptografia e segurança de redes”, Pearson Education do Brasil.

Valente, J. (2021) “Número de acessos móveis no Brasil cresce e fecha 2020 com 234 milhões”, https://agenciabrasil.ebc.com.br/geral/noticia/2021-04/numero-de-acessos-moveis-no-brasil-cresce-e-fecha-2020-com-234-milhoes, May/2021.

Wazlawick, R. S. (2014) “Metodologia de pesquisa para ciência da computação”, Elsevier.